Securing the Supply Chain

for Commercial off the Shelf (COTS) Industrial Automation and Control Devices and Systems Using ISA/IEC 62443 Standards

Andre Ristaino
Managing Director,
ISA Automation Standards Compliance Institute
aristaino@isa.org
919-990-9222
www.isasecure.org
67 TW Alexander Drive
Research Triangle Park, NC 27709
Founding Companies

- Siemens
  
  Ingenuity for life

- ExxonMobil

- Chevron

- BP

- Schneider Electric

- Yokogawa

- Honeywell

- Rockwell Automation

ISA99 Committee Liaison
Internationally Accredited ISO/IEC 17065 Conformance Scheme

ISASecure certification programs are supported by labs accredited to ISO/IEC 17065 and ISO/IEC 17025 lab operations by international ISO/IEC 17011 accreditation bodies (AB).

- Provides global recognition and acceptance of ISASecure certifications
- ISASecure can scale on a global basis using independent CB’s
- Independent ISO/IEC 17011 accreditation by global accreditation bodies ensures certification process is open, fair, credible, and robust.
- AB and CB agreements continue to expand.
ISO/IEC 17065 / ISO/IEC 17025 Accredited Certification Bodies

<table>
<thead>
<tr>
<th>ISASecure Certification Body</th>
<th>Accreditating Authority</th>
<th>Location(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exida, LLC</td>
<td>ANSI ANAB</td>
<td>Global operations – HQ Sellersville, PA USA</td>
</tr>
<tr>
<td>CSSC-CL</td>
<td>Japan Accreditation Board (JAB)</td>
<td>Japan and AP region- HQ Tokyo, Japan</td>
</tr>
<tr>
<td>TUV Rheinland</td>
<td>DAKkS</td>
<td>Global operations – HQ Cologne, Germany</td>
</tr>
</tbody>
</table>

Additional Certification Bodies are in Accreditation Process.
The first ISASecure chartered lab, accredited in 2011
CSSC-CL

Control Systems Security Corporation Tokyo & Tagajo City Japan
Why Certify COTS Products?

1. Security capabilities are independently assessed and certified by experts at accredited ISASecure labs

2. Reduces effort for end user to validate and verify security capabilities. (scarcity of talented cybersecurity expertise)

3. Objective metric for security capabilities based on industry standards. (hundreds of years of SME and knowledge codified into IEC 62443-x-x from hundreds of committee participants.)

One specification, one service mark, one assessment
Benefits and Value

End Users
• Simplifies specification process
• End users understand product capabilities
• Capabilities independently validated by external entity
• Confidence that security features will evolve over time

Equipment Vendors
Product Suppliers
• Differentiate solutions to marketplace
• Assurance products meet cybersecurity requirements
• Cybersecurity is a dimension of product quality
• Suppliers will soon face product liability accountabilities
Control Systems Security Lifecycle

Asset Owners
- Operate and Maintain
- Site Specific Systems

Integrators/Asset Owners
- Engineer and Integrate COTS
- into Site Specific Systems

Suppliers
- Design and Manufacture
- COTS Control Systems
ISA/IEC 62443 Standards Family

- **General**
  - ISA-62443-1-1: Terminology, concepts and models
  - ISA-TR62443-1-2: Master glossary of terms and abbreviations
  - ISA-62443-1-3: System security compliance metrics
  - ISA-TR62443-1-4: IACS security lifecycle and use-case

- **Policies & Procedures**
  - ISA-62443-2-1: Requirements for an IACS security management system
  - ISA-TR62443-2-2: Implementation guidance for an IACS security management system
  - ISA-TR62443-2-3: Patch management in the IACS environment
  - ISA-62443-2-4: Requirements for IACS solution suppliers

- **System**
  - ISA-TR62443-3-1: Security technologies for IACS
  - ISA-62443-3-2: Security levels for zones and conduits
  - ISA-62443-3-3: System security requirements and security levels

- **Component**
  - ISA-62443-4-1: Product development requirements
  - ISA-62443-4-2: Technical security requirements for IACS components

**Status Key**
- Published
- In development
- Planned
- Published (under review)
- Out for comment/vote
Three ISASecure® certifications available

1. Embedded Device Security Assurance (EDSA)  
   product certification  
   IEC 62443-4-2  
   IEC 62443-4-1

2. System Security Assurance (SSA)  
   product certification  
   IEC-62443-3-3  
   IEC 62443-4-1  
   IEC 62443-4-2

3. Security Development Lifecycle Assurance (SDLA)  
   process certification  
   IEC-62443-4-1
360 Degree Product Evaluation

- Product Development Process Audit
- Functional Security Capabilities Assessment
- Device Communication Robustness Test and Vulnerability Identification Scan

More than just testing!
# ISASecure EDSA Certified Devices

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Type</th>
<th>Model</th>
<th>Version</th>
<th>Level</th>
<th>Test Lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honeywell Process</td>
<td>Safety Manager</td>
<td>HPS 1009077 C001</td>
<td>R145.1</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>RTP Corporation</td>
<td>Safety manager</td>
<td>RTP 3000</td>
<td>A4.36</td>
<td>EDSA 2010.1 Level 2</td>
<td>exida</td>
</tr>
<tr>
<td>Honeywell Process Solutions</td>
<td>DCS Controller</td>
<td>Experion C300</td>
<td>R400</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Honeywell Process</td>
<td>Fieldbus Controller</td>
<td>Experion FIM</td>
<td>R400</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>RTP Corporation</td>
<td>Safety manager</td>
<td>RTP 3000</td>
<td>A4.36</td>
<td>EDSA 2010.1 Level 2</td>
<td>exida</td>
</tr>
<tr>
<td>Yokogawa</td>
<td>Safety Control System</td>
<td>ProSafe-RS</td>
<td>R3.02.10</td>
<td>EDSA2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Yokogawa Electric</td>
<td>DCS Controller</td>
<td>CENTUM VP</td>
<td>R5.03.00</td>
<td>EDSA 2010.1 Level 1</td>
<td>CSSC-CL</td>
</tr>
<tr>
<td>Hitachi, Ltd.</td>
<td>DCS Controller</td>
<td>HISEC 04/R900E</td>
<td>01-08-A1</td>
<td>EDSA 2010.1 Level 1</td>
<td>CSSC-CL</td>
</tr>
<tr>
<td>AZBIL (formerly Yamatake)</td>
<td>DCS Controller</td>
<td>Harmonas / Industrial-DEO / Harmonas-DEO</td>
<td>R 4.1</td>
<td>EDSA 2010.1 Level 1</td>
<td>CSSC-CL</td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>Field Process Controller</td>
<td>FCP280</td>
<td>S91061</td>
<td>EDSA 2010.1 Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>Tricon CX</td>
<td></td>
<td></td>
<td>EDSA 2020.1 Level 1</td>
<td>TUV Rheinland</td>
</tr>
<tr>
<td>Beijing Consen Technologies</td>
<td>Safety Related PES</td>
<td>TSxPlus V1.0</td>
<td>CM01-A-V001</td>
<td>EDSA v20 Level1</td>
<td>TUV Rheinland</td>
</tr>
<tr>
<td>HIMA Paul Hildebrandt GmbH</td>
<td>Safety Related PES</td>
<td>HIMAX X</td>
<td>CPU 01 FW Version 8.8 &amp; COM 01 FW Version 9.2</td>
<td>EDSA v2.0 Level T1</td>
<td>TUV Rheinland</td>
</tr>
<tr>
<td>TOSHIBA CORPORATION</td>
<td>DCS Controller</td>
<td>CIEMAC-DS/nv (TODIC-CIE DS/nv)</td>
<td></td>
<td>EDSA 2010.1 Level 1</td>
<td>CSSC-CL</td>
</tr>
</tbody>
</table>
ISASecure EDSA Certified Products
ISASecure EDSA Certified Products

TOSHIBA
Leading Innovation
## ISASecure SDLA Process Certified Development Organizations

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Locations</th>
<th>SDLA Version</th>
<th>Security Level (1-4)</th>
<th>Certification Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schneider-Electric</td>
<td>Foxboro, MA, USA</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider-Electric</td>
<td>Worthing, UK</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider-Electric</td>
<td>Lake Forest, CA USA</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider-Electric</td>
<td>Calgary AB, Canada</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Schneider-Electric</td>
<td>Hyderabad, India</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Honeywell Process</td>
<td>Phoenix, AZ</td>
<td>Version 1</td>
<td>SDLA Level 1</td>
<td>exida</td>
</tr>
<tr>
<td>Solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ISASecure Product Certificates
# ISASecure Recognized Test Tools

ISASecure test tool specifications and recognition process ensures that all test tools meet ISASecure requirements and provide consistent test outcomes.

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Product Name</th>
<th>Test Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable</td>
<td>Nessus</td>
<td>Vulnerability Identification Testing against US-CERT NVDB</td>
</tr>
<tr>
<td>Beyond Security</td>
<td>beSTORM EDSA</td>
<td>CRT, SRT and network robustness</td>
</tr>
<tr>
<td>Hitachi</td>
<td>Raven</td>
<td>CRT, SRT and network robustness</td>
</tr>
<tr>
<td>Synopsys</td>
<td>Defensics X</td>
<td>CRT, SRT and network robustness</td>
</tr>
<tr>
<td>Wurldtech</td>
<td>Achilles Satellite</td>
<td>CRT, SRT and network robustness</td>
</tr>
<tr>
<td>CNCERT/CC &amp; Beijing Xinlian Kehui</td>
<td>Acheron 2.2</td>
<td>CRT, SRT, and network robustness</td>
</tr>
<tr>
<td>Technology Co., LTD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2016 ISASecure Building Control Systems Working Group

Participating Organizations

Schneider Electric
CSA Group
Johnson Controls

Maverick Technologies
Honeywell
Siemens

George Brown College
RBCG
Syska Hennessy Group

ISA Security Compliance Institute
CABA

Mike Chipley-PMC Group, LLC
Jim Sinopoli-Smart Buildings, LLC

Download Working Group Final Report at
ISASecure Certification Growth